Don't Repeat Yourself: Automatically Synthesizing Client-side Validation Code for Web Applications

Nazari Skrupsky, **Maliheh Monshizadeh**, Prithvi Bisht, Timothy Hinrichs, V.N. Venkatakrishnan, Lenore Zuck

UIC University of Illinois at Chicago
Department of Computer Science

Overview

- Introduction
- Goals, Challenges
- Our Approach
- WAVES Tool
- Results
- Conclusion

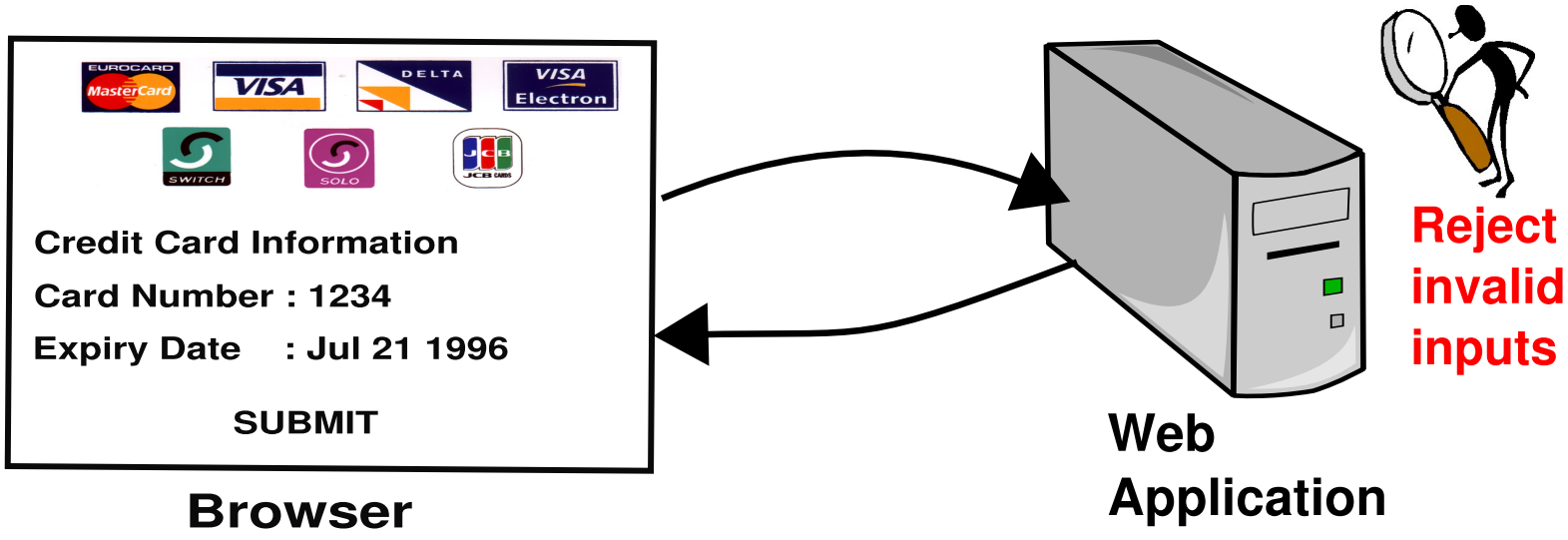
Introduction

- Web Application Development
  - ✦ Client-side
    - HTML, JavaScript, ...
  - ✦ Server-side
    - PHP, Java, ASP

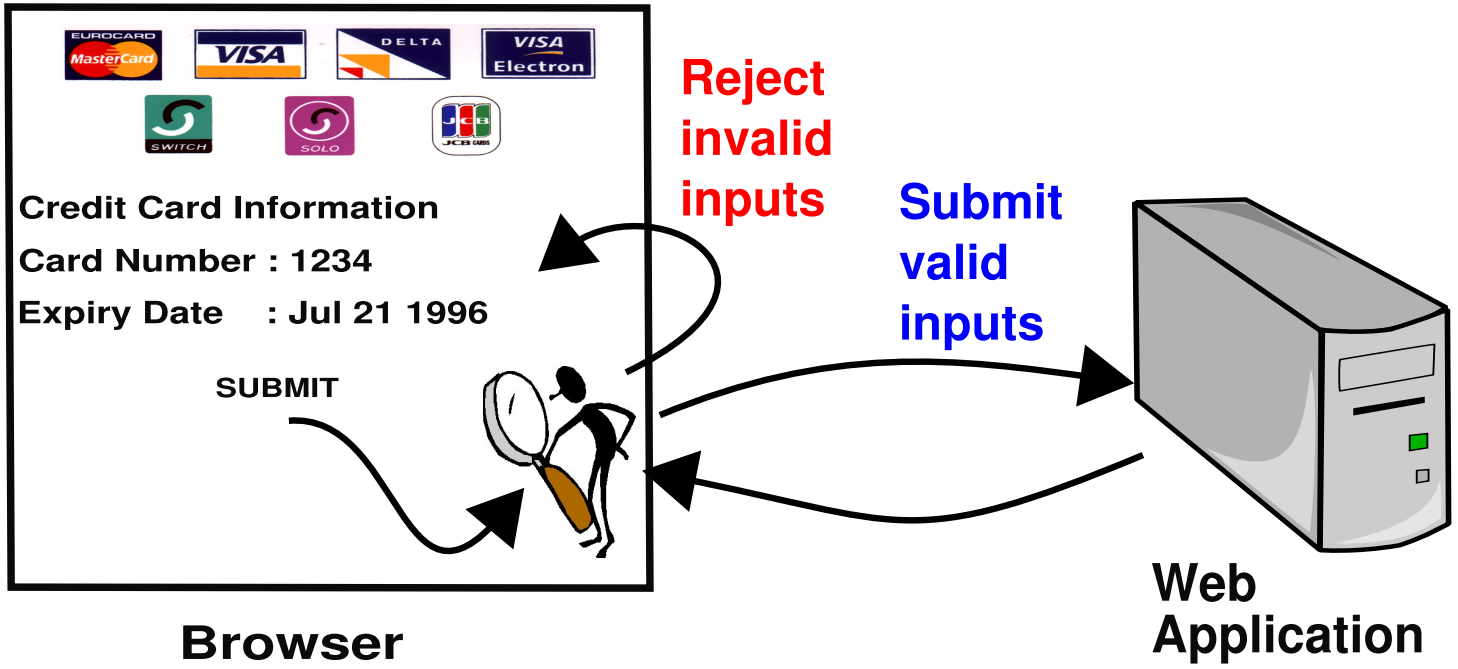
➡ Independent development is **problematic**

- When the client and server share application logic

Input Validation



Parameter Tampering



➡ **Input validation must always occur at the server**

WAVES

(Web Application Validation Extraction and Synthesis)

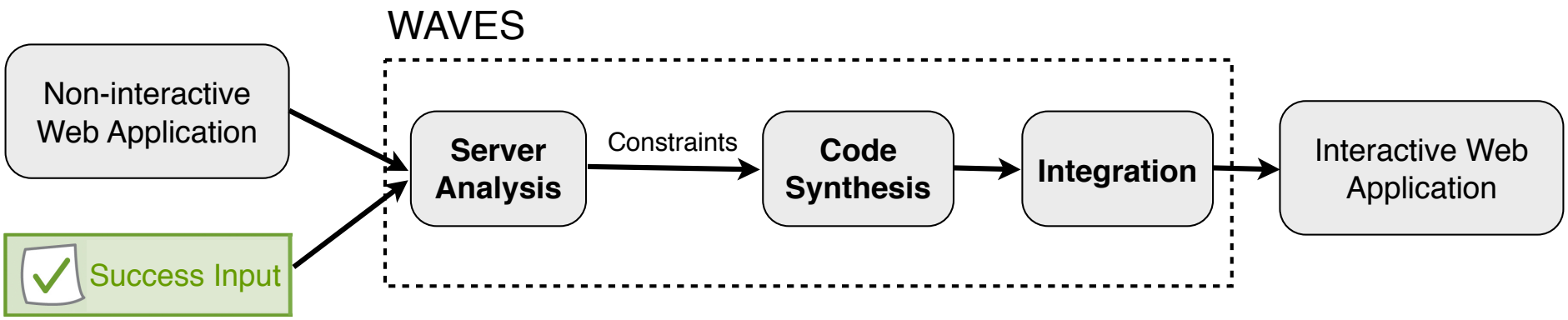
- Automatic synthesis of **input validation** for client-side
- Benefits:
  - Development **Efficiency**
  - Greater **Compatibility**
  - Code Efficiency

Automatic Synthesis

Challenges

- Inference of server-side constraints
  - Server-side: Variables
  - Client-side: Form Fields
- Preservation of application **logic** and **security**
- Validation involving the server state

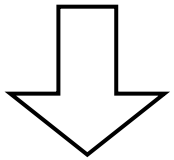
WAVES Architecture



WAVES

1- Server Analysis

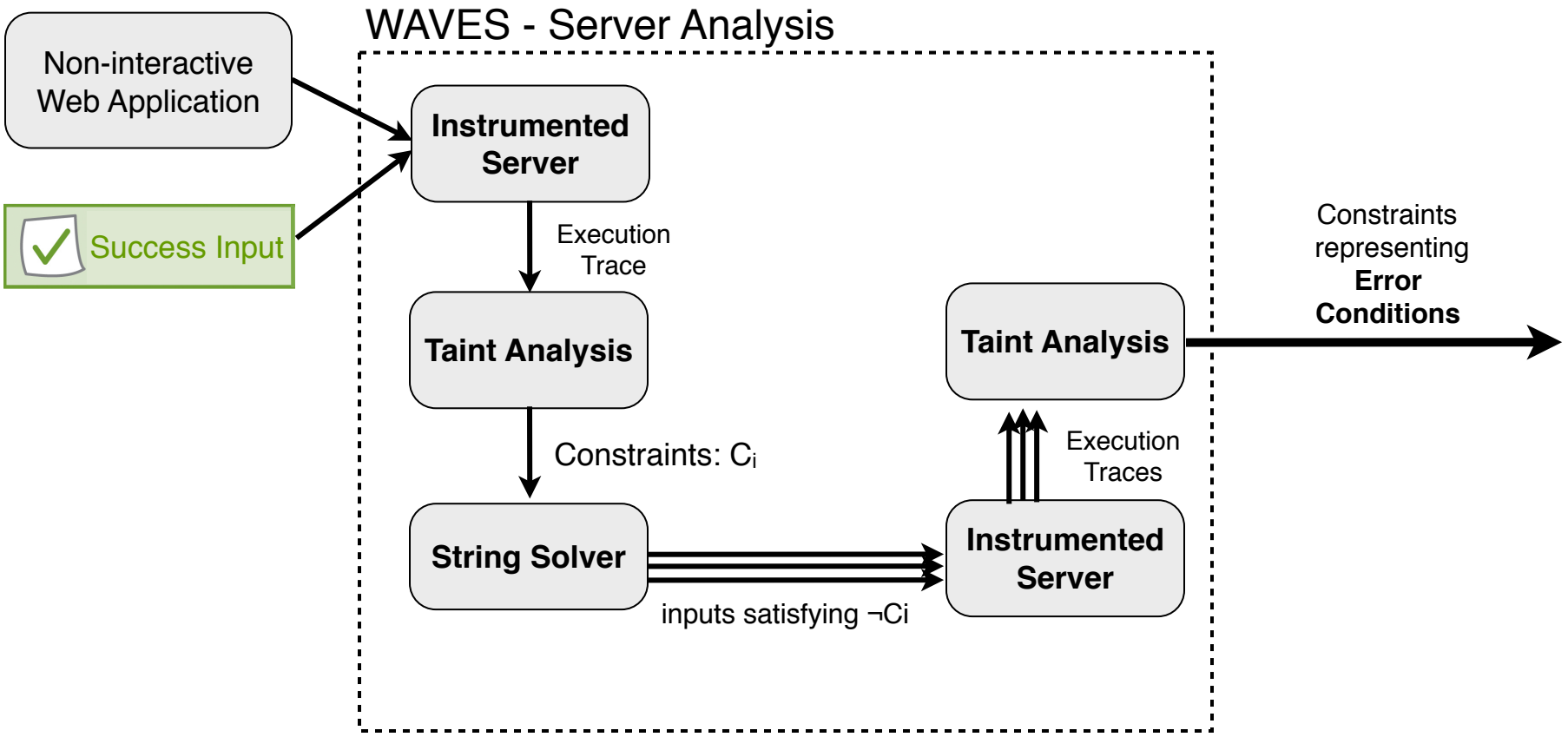
$F_{\textbf{server}}$ = All conditions on user inputs that must be satisfied to reach sensitive operations



1. Submit benign inputs
2. Extract server formula

WAVES

1- Server Analysis



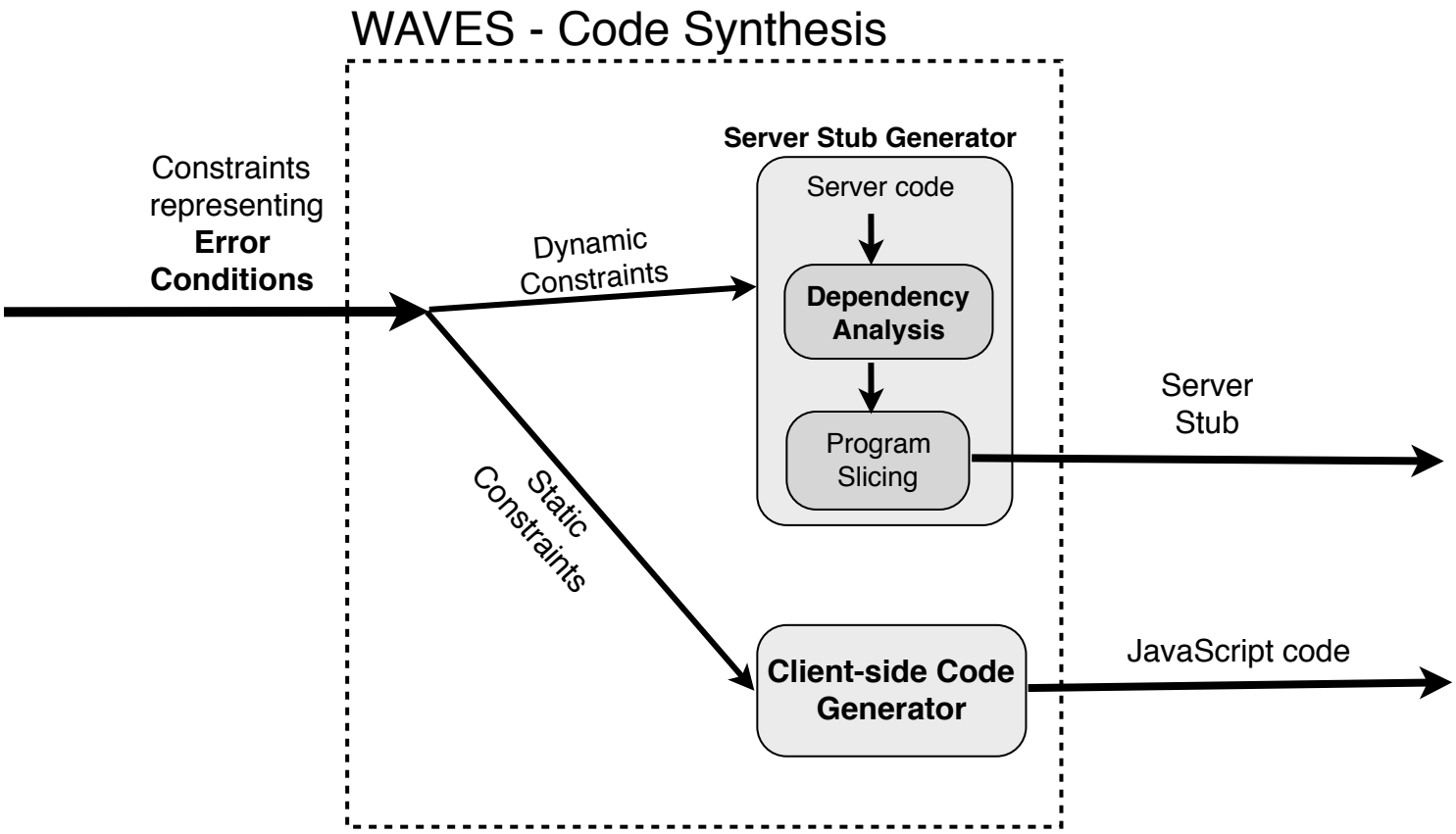
WAVES

2- Synthesis

- Static Constraints
  - pass1 == pass2
- Dynamic Constraints: **Dependent** on the server state
  - userID is UNIQUE

WAVES

2- Synthesis



Results

- Three **medium to large** and popular PHP applications
  - B2Evolution
  - WeBid
  - WebSubRev
- Successfully synthesized **83%** of the constraints
- Generated Stubs are **much smaller** (less than **26%**)
- Improved **RTT 43 to 164 ms** (originally 65 to 633 ms)

Conclusion

- Code efficiency
- Interactive applications
- Improved performance

Related Papers

1) Prithvi Bisht, Timothy Hinrichs, Nazari Skrupsky, and V. N. Venkatakrishnan. **"WAPTEC: Whitebox Analysis of Web Applications for Parameter Tampering Exploit Construction"**. In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11). ACM, New York, NY.

2) Prithvi Bisht, Timothy Hinrichs, Nazari Skrupsky, Radoslaw Bobrowicz, and V. N. Venkatakrishnan. **"NoTamper: Automatic Blackbox Detection of Parameter Tampering Opportunities in Web Applications"**. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). ACM, New York, NY.

Questions?